UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/240,265	01/29/1999	MARK E. PETERS	CR9-98-095	7166

25259 7590 03/23/2006

IBM CORPORATION
3039 CORNWALLIS RD.
DEPT. T81 / B503, PO BOX 12195
REASEARCH TRIANGLE PARK, NC 27709

EXAMINER	
CALLAHAN, PAUL E	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 03/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/240,265	PETERS, MARK E.	
	Examiner	Art Unit	
	Paul Callahan	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 March 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 March 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 3/3/06 has been entered.

2. Claims 1-12 are pending in this application and have been examined.

Response to Arguments

3. Applicant's arguments filed 3-3-06 have been fully considered but they are not persuasive.

The applicant argues in traverse of the rejection of the claims as found in the previous [final] Office Action by asserting that the applied references do not teach the feature of a signature associated with each public key as called for in the independent claims. Yet as the applicant acknowledges, the admitted prior art of RFC 2459 at 4.1.2.9 does teach an X.509 certificate having such features. In addition Balenson does teach this feature in Sec. 4.3 as noted previously.

The Applicant argues that Schneier fails to teach the use of extensions in a X.509 certificate, yet it does so implicitly by referencing the fields containing the extensions of a standard X.509 certificate.

The Applicant argues that Shambroom fails to teach authenticating a device via an alternative listed algorithm. Yet such a limitation, directed towards device authentication, is not found in the claims.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 1-3 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Changes have been made via the latest amendment to the language of claim 1 by the addition of language directed towards execution on computer apparatus. However it is not clear from the language of the claims how the X.509 certificate can be considered as executable code capable of causing a change in a computer apparatus. The X.509 certificate is in fact mere data that another program may act upon when it is read out from the memory medium. Claims 1-3 claim data, which is nonfunctional descriptive material. As such, embodying the data on a computer-readable would not make the claims statutory without language directed to read-out and execution of computer code so as to cause a computing device to execute the steps coded for. See MPEP 706.03(a) and, especially, 2106 IV B 1 (b).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shambroom (5923756) and Schneier Applied Cryptography, in view of Balenson, "Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers", Network Working Group, Request For Comments (RFC) 1423, February 1993.

As for claim 1, in lines 32-35 of column 10, Shambroom discusses a certificate that includes a public key and list of one or more cryptographic algorithms supported by the entity associated with the public key. The certificate can resemble an X.509 certificate. On pages 574 and 575, Schneier describes the X.509 certificate. As can be seen in figure 24.2, the certificate includes a section (certificate extension) that identifies the algorithm, parameters, and a public key. There is also a section for a signature. These read on the first clause of applicant's first claim as amended. The list of algorithms disclosed in Shambroom also anticipates an extension for identifying at least one alternative algorithm. Shambroom does not dictate that a second public key and signature therefore be included in the certificate or used as an alternative means of protecting data included within the certificate. However Balenson does explicitly teach

this (certificate extension) feature in Section 4.3, Asymmetric Signature Algorithms. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to configure an X.509 certificate to utilize alternative signatures formed with different algorithms on data contained within the certificate as taught by Balenson, in the exemplary X.509 certificate of Shambroom and Schneier, thereby protecting the data from compromise. It would have been desirable to do so since utilization of alternative algorithms would increase the difficulty in unauthorized access to the protected data within the certificate. Motive to make this combination is found for example, at page 574 where Schneier discusses the advantages of X.509 certificates capable of utilizing different algorithms such that authentication across networks is made possible.

As for claim 2, pages 480 and 481 of Schneier discuss elliptic curve public key systems. RSA is first mentioned on page 17. According to Schneier, it is the most popular public-key algorithm. There are trade-offs between the two, particularly in terms of the relative computational workloads of the two entities (signer and verifier). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to support RSA and an elliptic curve cryptosystem with the X.509 certificate taught by Shambroom.

As for claim 3, both of the signatures taught by the combination of Shambroom, Schneier and Balenson verify at least part of the certificate and hence read on claim 3.

Claims 4-6, 7-9, and 10-12 contain substantially the same limitations as do claims 1-3, and are therefore rejected on the same grounds.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Emmanuel Moise, can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is: (571) 273-8300.

3-10-06

Paul Callahan

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER